**Your Organization Logo Here**

# Organization XYZ Outsourcing Policy

## 1.0 Purpose

The purpose of this policy is to establish the requirements for identifying, justifying, and implementing outsourcing arrangements for any Organization XYZ function.

## 2.0 Scope

This policy applies to all workforce members within Organization XYZ. It must be followed whenever Organization XYZ functions are outsourced.

## 3.0 Policy

To conduct operations as effectively and efficiently as possible, Organization XYZ may find it advantageous to outsource (use outside contractors for) certain functions. To ensure compliance with security objectives, these requirements must be followed:

### 3.1 Board and Management Responsibility

3.1.1 The Board and senior management are responsible for ensuring that adequate risk mitigation practices are in place for the effective oversight and management of outsourcing arrangements.

3.1.2 The Board, or delegated committee should:

a) approve all outsourcing arrangements of material business activities;
b) review and approve risk management policies for outsourcing, including ensuring an appropriate exit strategy is in place;
c) regularly review compliance with the outsourcing policy; and
d) regularly review reports on outsourcing arrangements and be informed on the performance of the service provider.

3.1.3 In managing the outsourcing arrangement, senior management should:

a) develop a risk management framework for outsourcing arrangements that reflects the Board approved policy;
b) be involved in the due diligence process, evaluation and selection of potential service providers;
c) establish and implement an oversight process that ensures that outsourcing arrangements, and outsourcing of material business activities in particular, are reported to the Board prior to implementation;
d) ensure that, for each outsourcing arrangement, there is a formal evaluation of the service provider, that a contract with appropriate service level agreements (SLAs) is in place, and




mmenninger@runbox.com

that confidentiality provisions and security needs are adequately addressed; and

e) ensure that appropriate reporting is place to enable effective management and control of outsourcing arrangements and to identify potential problems at an early stage.

### 3.2 Risk Mitigation Strategies: Outsourcing Team

3.2.1 When outsourcing material business activities, Organization XYZ will consider establishing an outsourcing team comprised of individuals from both the business area proposing the outsourcing arrangement and other individuals with the necessary skills to assess the risks involved in outsourcing. This may include specialists in the relevant risk areas and may involve using external experts.

3.2.2 This team should ensure that the Board approved policy on outsourcing is being followed at all times, including the due diligence processes, evaluation of the outsourcing options and the making of recommendations to senior management and the Board.

### 3.3 Business Case

3.3.1 A detailed business case should be prepared, detailing the potential costs, benefits and risks associated with the proposed outsourcing arrangement.

3.3.2 As part of this process, the Board should be making an "in principle" decision to continue the outsourcing process and to call for Requests for Proposal (RFPs) or other selection process documents. The RFPs should clearly outline the requirements of Organization XYZ for the proposed outsourcing arrangement.

### 3.4 Due Diligence

3.4.1 The due diligence process should always be undertaken prior to any final decision being made as to whether to outsource a material business activity. This should address all material factors that would impact on the potential service provider's ability to perform the business activity.

3.4.2 The due diligence process should, as a minimum, assess the financial ability, technical ability and capacity of the service provider to deliver, including in stress situations, the required services.

3.4.3 The evaluation process should include an assessment of the service provider's control framework, covering performance standards, policies, procedures, compliance, reporting and monitoring processes.

3.4.4 The due diligence should also address other issues, such as business strategy, reputation, experience with the proposed

outsourced function, reliance on and performance of external service providers, insurance coverage, business continuity management (BCM), and potential conflict of interest where the service provider is related to Organization XYZ or has arrangements with competitors.

### 3.5 Business Continuity Management (BCM)

Where a material business activity is outsourced, Organization XYZ should ensure that the BCM documentation outlines the procedures to be followed in the event that the service provider is unable to fulfill its obligations under the outsourcing agreement for any reason.

### 3.6 Contractual Agreements

3.6.1 All material outsourcing arrangements must be undertaken using a written, legally binding agreement. The agreement must document all components of the outsourcing arrangement between the parties. Organization XYZ should obtain legal advice in assessing the contract.

3.6.2 The agreement should be for a specified period and contain both start and finish dates. There should also be a clause allowing for periodic review of the agreement within the term of the contract and renegotiation if appropriate.

3.6.3 The contract should specify the content, frequency and format of the service being provided. It should state timelines for receipt and delivery of work, including specifying priorities. It should contain performance benchmarks, including default benchmarks which, if not met, would result in penalties being applied or, in the extreme, termination of the agreement. The agreed service levels should be specified in SLAs.

3.6.4 The contract should specifically cover any subcontracting or outsourcing by the service provider, including any specific rules or limitations to such arrangements (for example notification to Organization XYZ prior to entering into a subcontracting arrangement). In particular, the same standards that apply to the service provider in respect to security and confidentiality of information, offshoring, compliance with relevant legislation and regulations, and Organization XYZ access to information, should apply to sub-contractors or outsourcing arrangements by the primary service provider.

3.6.5 The contract should be sufficiently flexible to accommodate changes to existing processes and to anticipate new processes in the future.

3.6.6 The contract should clearly set out the procedures in place to allow Organization XYZ to effectively monitor the performance of the service provider. This would include the extent to which Organization XYZ's internal or external auditors can obtain

sufficient information (including through on-site inspections or the appointment of an external party) to satisfy themselves of the adequacy of risk management systems. Consideration should also be given to contract provisions requiring an annual review of the service provider's internal control systems by an independent expert.

3.6.7 The contract should include clauses enabling Organization XYZ to access documentation related to the outsourcing arrangement, and to conduct on-site visits to the service provider. This should include arrangements for Organization XYZ to meet directly with the service provider, and for the service provider to cooperate with Organization XYZ's requests for information and assistance.

3.6.8 The contract must include details covering BCM to ensure that acceptable service levels are maintained in the event of problems occurring with the service provider. The contract should also ensure that this requirement applies to any sub-contracting or outsourcing by the service provider.

3.6.9 With respect to default arrangements, the contract should clearly specify what constitutes a default event, identify how these are to be rectified and specify any indemnity provisions.

3.6.10 The circumstances that would lead to a termination of the outsourcing arrangement should be clearly specified in the contract. It should set out possible reasons for terminating the arrangement and procedures to be followed in the event of termination, including notice periods, the rights and responsibilities of the respective parties and transition arrangements. The latter would address access to, and ownership of, documents, records, software and hardware. Termination clauses should also specify the time period over which the business activity continues to be undertaken by the service provider and its role in transitional arrangements should the activity be brought back in-house within Organization XYZ or outsourced to another service provider.

3.6.11 The contract should set out explicit pricing arrangements, covering issues such as frequency of payment, invoicing and payment procedures.

3.6.12 Formal dispute resolution mechanisms should be incorporated into the contract. These mechanisms would define procedures for managing disputes. They would enable the continued operation of the outsourced activity while specific issues are being dealt with, including conciliation and arbitration arrangements.

3.6.13 The contract should specify the extent of liability for each party and, in particular, whether liability for negligence is limited. It should specify any indemnities and provide details of any insurance arrangements.

3.6.14 The contract should include specific provisions for outsourcing to service providers conducting the outsourced activity from outside the United States (or outside of the country where Organization XYZ's headquarters are located).

### 3.7 Management and Control of the Outsourcing Relationship

3.7.1 Whenever Organization XYZ undertakes a material outsourcing arrangement, procedures to monitor and control outsourcing risk should be put in place in accordance with the Board approved policy. The actual reporting framework, to both the Board and senior management, should reflect the size and nature of the arrangements. Accountability for managing the outsourcing arrangement should be specifically assigned to an individual or team/committee. This ensures that there is likely to be continued focus on the outsourcing arrangement.

3.7.2 The Board (or delegated committee) and senior management should receive regular reports on outsourcing activities. Any material problems with outsourcing should be brought to the attention of these parties.

3.7.3 This monitoring process could involve the use of internal (or, where considered relevant or more appropriate, external) audit to ensure compliance with outsourcing policies and procedures. The audit function can be used to:

a) ensure compliance with risk management policies and procedures;
b) ensure appropriate internal controls are in place; and
c) ensure that reporting is adequate, accurate and timely.

3.7.4 Organization XYZ should ensure that records held by the service provider are adequate for audit trail purposes and that those records held by the service provider are readily available at all times to Organization XYZ.

### 3.8 Offshoring

3.8.1 In addition to the general due diligence process outlined in 3.4, Organization XYZ, in assessing whether to approve an application to offshore a material business activity, would expect the Board to consider the risks which arise from offshoring, including:

a) country risk - the risk that overseas economic, political and/or social events will impact upon the ability of the overseas service provider to continue to provide an outsourced service to Organization XYZ;
b) compliance (legal) risk - the risk that offshoring arrangements will impact upon Organization XYZ's ability to comply with relevant United States and overseas laws and regulations (including accounting practices);

c) contractual risk - the risk that Organization XYZ's ability to enforce the offshoring agreement may be partly or completely hindered;
d) access risk - the risk that the ability of Organization XYZ to obtain information and to retain records may be partly or completely hindered. This risk also refers to the potential difficulties or inability of Organization XYZ to access the service provider and the material business activity being conducted; and
e) counterparty risk - the risk arising from the service provider's failure to meet the terms of any contract with Organization XYZ or to otherwise perform as agreed.

3.8.2 These and other additional risks should be specifically addressed during the preparation of a business case, when conducting the due diligence, and during contract negotiations. Where Organization XYZ approves the offshoring arrangement, these risks should also be considered when conducting the ongoing monitoring and control of that material business activity. Specific risk management expertise is required when assessing, monitoring and controlling material business activities outsourced to service providers conducting the activities outside the United States.

3.8.3 Organization XYZ should also consider the addition of provisions in the outsourcing agreement, to include (but not be limited to):

a) Choice of law - Contracts should specify under which particular jurisdiction contractual disputes will be resolved. The due diligence process should include an examination of the relevant overseas legislation and regulations by a suitably qualified expert to ensure that contractual provisions are recognized by the overseas jurisdiction and are able to be enforced in the chosen jurisdiction;
b) Security and confidentiality of information - Organization XYZ should ensure that contractual provisions in relation to data are of the same standard as those required of a domestic service provider and in accordance with requirements under U.S. legislation and regulations. Contracts should also ensure that all information forwarded to the service provider by Organization XYZ (as well as any information forwarded by the service provider to third parties in the course of providing that service, such as to a back-up disaster recovery provider) remains the property of Organization XYZ; and
c) Access to information/persons - Any agreement with a service provider should not restrict access to information by Organization XYZ or external auditors, independent third parties or representatives of Organization XYZ for the purposes of confirming the performance of the risk management systems. Legal due diligence undertaken prior to the execution of the contract should also ensure that there no legal impediments to Organization XYZ's access to information and/or relevant persons employed by Organization XYZ or

service provider for the purposes of examining the organization in relation to the regulation of the Organization XYZ's activities.

3.8.4 Records should be maintained by Organization XYZ in a United States office, and in English. These records should include (but not be limited to):

a) a copy of the contractual agreement;
b) a copy of the due diligence assessment;
c) a copy of the service provider's BCM documentation and details of the latest testing of BCM processes undertaken; and
d) copies of financial statements, reports and any other information Organization XYZ considers critical to the ongoing monitoring and control of the outsourcing arrangement with the service provider.

3.8.5 Due to additional risk management issues specific to offshoring, Organization XYZ should ensure ongoing monitoring of economic, social and political conditions within the host country to assess the ability of the service provider to continue to adequately perform the contracted service. Organization XYZ should also consider specific contingency plans in the event that the service provider is unable to continue to provide the outsourced service. The contingency plan would normally include the identification of an alternate service provider and/or requirements in the eventuality that the outsourced activity needed to be brought back within Organization XYZ.

### 3.9 Final Approval

Decisions to outsource material business activities should be approved or endorsed by the Board or delegated committee.

## 4.0 Responsibilities

**4.1** The Board or delegated committee is responsible for ensuring that the outsourcing policy is followed.

## 5.0 Compliance

**5.1** Company officers and senior management are required to ensure that internal audit mechanisms exist to monitor and measure compliance with this policy.
**5.2** Failure to comply with this policy may result in disciplinary action, which may include termination of employment.

## 6.0 Definitions

**Outsourcing:** procuring of services or products from an outside supplier or manufacturer in order to cut costs.

**Offshoring:** relocation of business processes from one country to another. This includes any business process such as production, manufacturing, or services.




mmenninger@runbox.com

## 7.0 Related Policies and Standards

- Corporate Security Policy

## 8.0 Revision History

| Version | Date | Revision |
|---|---|---|
| 1.0 | Month Day, Year | Policy Written |




mmenninger@runbox.com